UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,665	10/10/2003	James Edward Aston	RSW920030166US1	1807

7590 05/29/2007

David R. Irvin
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/683,665	**Applicant(s)** ASTON ET AL.	
	Examiner Tongoc Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/2/2003*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's Application filed on 10/10/2003. Claims 1-29 are pending for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 10/2/2003 has been considered by the Examiner.

Oath/Declaration

3. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

It does not state that the person making the oath or declaration has reviewed and understands the contents of the specification, including the claims, **as amended by any amendment specifically referred to in the oath or declaration.**

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

> applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5, 6, 8. 11, 12, 14, 15, 17, 20, 21, 23, 24, 25 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Hypponen et al. (U.S. Patent No. 6, 577, 920, hereinafter Hypponen).

With respect to claims 1, 11 and 20, Hypponen discloses a computer system, method and a computer-readable medium whose contents cause a computer system to perform selective virus signature scanning against a target file associated with an executing agent, the computer system having an anti-virus program with instructions to perform the steps of (Abstract):

organizing virus signatures into a plurality of anti-virus sets where each set contains a characteristic shared by all the virus signatures within the set (e.g. col. 3, lines 14-20); associating a portion of the plurality of anti-virus sets with the executing agent (e.g. col. 3, lines 14-20, col. 4, lines 50-55); and scanning the contents of the target file for a virus signature which matches a virus signature stored in the associated one or more anti-virus sets (e.g. col. 3, lines 50-52).

With respect to claims 2, 12 and 21, Hypponen further discloses comprising a step before the scanning step, the step comprising: associating a rule with the executing agent to indicate a manner in which the associated portion of the plurality of anti-virus sets are applied (e.g. col. 5, lines 23-31).

With respect to claims 3 and 23, Hypponen further discloses wherein the associating step includes providing user selectable options (e.g. col. 5, lines 19-22).

With respect to claims 5, 14 and 24, Hypponen further discloses wherein the manner in which the associated portion of the plurality of anti-virus sets are applied to executing agent's target files includes a trigger mechanism which invokes subsequent scanning of the executing agent's target files (e.g. col. 4, lines 28-54).

With respect to claims 6, 15 and 25, Hypponen further discloses wherein the trigger mechanism includes applying the scanning step upon a request for a file operation on the target file (e.g. col. 4, lines 37-42).

With respect to claims 8, 17 and 27, Hypponen further comprising a step before the organizing step, the step comprising: determining the plurality of executing agents installed on the computer system (e.g. col. 3, lines 3-5).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 7, 13, 16, 22 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen (U.S. Patent No. 6,577,920) in view of Sarkar (U.S. Patent Application Publication No. 2004/0158730).

With respect to claims 4, 13 and 22, Hypponen does not disclose wherein the rule applied includes a periodic batch scan of one or more target files. However, Sarkar discloses an anti-virus system performing batch mode scanning according to a periodic job scheduler (e.g. Sarkar, [0064]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement file screening protection by grouping macro virus signatures into different databases taught by Hypponen with periodic batch scanning according to job schedule taught by Sarkar as part of file protection maintenance.

With respect to claims 7, 16 and 26, Hypponen does not disclose wherein the trigger mechanism includes applying the scanning step periodically on one or more target files associated with the executing agent. However, Sarkar discloses a set of program instruction in a program module invoking file scanning for anti-virus protection according to periodic job schedule (Sarkar, [0064]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement file screening protection by grouping macro virus signatures into different databases taught by Hypponen with a program module to invoke periodic scanning according to job schedule taught by Sarkar as part of file protection maintenance.

6. Claims 9, 10, 18, 19, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen (U.S. Patent No. 6,577,920) in view of Vaidya (U.S. Patent No. 6,279,113).

With respect to claims 9, 10, 18, 19, 28 and 29, Hypponen discloses wherein the plurality of anti-virus sets have a first anti-virus set and a second anti-virus set, Hypponen further discloses the organizing step further comprises:

arranging the plurality of anti-virus sets into a hierarchical structure having first and second levels, the first level having the first anti-virus set containing virus signatures which are mutually applicable to a plurality of executing agents (e.g. col. 3, lines 17-20), Hypponen does not explicitly describe the second level having the second anti-virus set containing virus signatures which are exclusively applicable to the first portion of the plurality of executing agents or a third level having the third anti-virus set containing virus signatures which are exclusively applicable to one of the first portion of the plurality of executing agents.

. However, Hypponen describe a type of virus consisted of a piece of executable code which attached itself to a bona fide computer program that typically inserted a JUMP instruction into the start of the program which when the program was executed, caused a jump to occur to the "active" part of the virus (Hypponen, col. 1, lines 15-19). Vaidya discloses a dynamic signature-based network intrusion detection system includes multiple attack signature profiles which are each descriptive of identifiable characteristic associated with particular network intrusion attempts associated with network objects located on the network, the attack signature profiles can include *generic attack and/or* *customized attack signature profile* (e.g. Vaidya, col. 3, lines 12-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Hypponen's describing a certain virus that attach *in the start of a program* to trigger the virus code to activate in a software program with Vaidya's teaching of generic and/or customizing attack signature into different signature profiles to improve the virus detection system in way that efficiently associating identifiable characteristic with particular network intrusion attempts and network objects (Vaidya, col. 3, lines 34-38).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Shanklin et al. disclose intrusion detection signature analysis using regular expressions and logical operations.

-Chen et al. disclose event triggered iterative virus detections

-Kephart et al. disclose efficient detection of computer viruses and other data traits.

-Wells discloses method and apparatus for computer virus detection, analysis, and removal in real time.

Shieh et al. disclose a pattern-oriented intrusion-detection system and method.

-Edwards discloses a method and system for limiting processor utilization by a virus scanner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Examiner: Tongoc Tran
AU: 2134

May 14, 2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER